

Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): In a data communication network, a method for protecting a node, said method comprising processes of:

identifying a said node to be protected;

allocating a primary bandwidth pool on links of said data communication network for use by primary paths;

providing allocating a backup bandwidth pool on said links of said data communication network for use as a backup, said backup bandwidth pool on each of said links comprising a bandwidth equal to at least a link speed minus a maximum reservable bandwidth for said primary paths on said link;

identifying a link pair traversing said node to be protected, said link pair having a bandwidth to be protected;

establishing as a backup for said link pair a set of one or more backup paths that do not include said node and wherein said one or more backup paths collectively have backup bandwidth greater than or equal to said bandwidth to be protected;

deducting, for each link included in said set of paths, from backup bandwidth available for protecting said node, while not deducting from backup bandwidth available for protecting other nodes in said data communication network; and

repeating said processes of identifying, establishing, and deducting for a plurality of link pairs traversing said node without exceeding available backup bandwidth of links used in establishing said backups;

wherein said bandwidth to be protected of said link pair comprises a lesser of primary bandwidths of links of said link pair traversing said node to be protected.

Claim 2 (canceled).

Claim 3 (canceled).

Claim 4 (original): The method of claim 1 wherein said set of one or more paths comprises one or more label switched paths.

Claim 5 (original): The method of claim 1 wherein said processes of identifying and establishing occur under control of said node.

Claim 6 (original): The method of claim 1 wherein said processes of identifying and establishing occur under control of a computer independent of said node.

Claim 7 (original): The method of claim 1 further comprising:
signaling said backups to other nodes adjacent to said node in said data communication network.

Claim 8 (currently amended): A method for operating a data communication network to provide protection to nodes in said data communication network, said method comprising:

maintaining, for each of a plurality of links in said data communication network, a primary bandwidth pool for use by primary paths and a backup bandwidth pool for use by backup tunnels; and

establishing said backup tunnels to protect a plurality of nodes of said network, each of said backup tunnels consuming backup bandwidth from backup bandwidth pools of selected ones of said plurality of links; and

wherein all backup tunnels protecting any particular node of said network do not consume more bandwidth on any link than provided by the link's backup bandwidth pool but wherein there is at least one set of backup tunnels that protect disparate nodes and that consume more bandwidth on at least one link than provided by said at least one link's backup bandwidth pool, and

wherein establishing backup tunnels comprises signaling said backup tunnels with zero bandwidth to adjacent nodes of each protected node.

Claim 9 (original): The method of claim 8 wherein at least one of said backup tunnels comprises a label switched path.

Claim 10 (canceled).

Claim 11 (original): The method of claim 8 wherein establishing backup tunnels comprises:

performing backup tunnel selection computations at each protected node for that protected node.

Claim 12 (canceled).

Claim 13 (canceled).

Claim 14 (canceled).

Claim 15 (canceled).

Claim 16 (currently amended): In a data communication network, a computer program product for protecting a node, said computer program product comprising:

code that identifies said node to be protected;

code that allocates a primary bandwidth pool on links of said data communication network for use by primary paths;

code that establishes allocates a backup bandwidth pool on said links of said data communication network for use as a backup, said backup bandwidth pool on each of said links comprising a bandwidth equal to at least a link speed minus a maximum reservable bandwidth for said primary paths on said link;

code that identifies a link pair traversing said node to be protected, said link pair having a bandwidth to be protected;

code that establishes a backup for said link pair a set of one or more backup paths that do not include said node and wherein one or more backup paths collectively have backup bandwidth greater than or equal to said bandwidth to be protected;

code that deducts, for each link included in said set of paths, from backup bandwidth available for protecting said node, while not deducting from backup bandwidth available for protecting other nodes in said data communication network;

code that repeatedly invokes said code that identifies, establishes, and deducts for a plurality of link pairs connected to said node without exceeding available backup bandwidth of links used in establishing said backups; and

a computer-readable storage medium that stores the codes;

wherein said bandwidth to be protected of said link pair comprises a lesser of primary bandwidths of links of said link pair traversing said node to be protected.

Claim 17 (canceled).

Claim 18 (canceled).

Claim 19 (original): The computer program product of claim 16 wherein said set of one or more paths comprises one or more label switched paths.

Claim 20 (original): The computer program product of claim 16 further comprising:

code that signals said backups to other nodes adjacent to said node in said data communication network.

Claim 21 (currently amended): A computer program product for operating a data communication network to provide protection to nodes in the data communication network, said computer program product comprising:

code that maintains, for each of a plurality of links in said data communication network a primary bandwidth pool for use by primary paths and a backup bandwidth pool for use by backup tunnels; and

code that establishes said backup tunnels to protect a plurality of nodes of said network, each of said backup tunnels reserving backup bandwidth from backup bandwidth pools of selected ones of said plurality of links;

wherein all backup tunnels protecting any particular node of said network do not consume more bandwidth on any link than provided by the link's backup bandwidth pool but wherein there is at least one set of backup tunnels that protect disparate nodes and that consume more bandwidth on at least one link than provided by said at least one link's backup bandwidth pool; and

wherein code that establishes backup tunnels comprises code that signals said backup tunnels with zero bandwidth to adjacent nodes of each protected node; and
a computer-readable storage medium that stores the codes.

Claim 22 (original): The computer program product of claim 21 where at least one of said backup tunnels comprises a label switched path.

Claim 23 (canceled).

Claim 24 (original): The computer program product of claim 21 wherein said code that establishes backup tunnels comprises:

code that performs backup tunnels selection computation at each protected node for that protected node.

Claim 25 (currently amended): A network device for implementing a node in a data communication network, said network device comprising:
a processor; and

a memory storing instruction for said processor, said instructions comprising:

code that identifies said node to be protected;

code that allocates a primary bandwidth pool on links of said data communication network for use by primary paths;

code that establishes allocates a backup bandwidth pool on said links of said data communication network for use as a backup, said backup bandwidth pool on each of said links comprising a bandwidth equal to at least a link speed minus a maximum reservable bandwidth for said primary paths on said link;

code that identifies a link pair traversing said node to be protected, said link pair having a bandwidth to be protected;

code that establishes a backup for said link pair a set of one or more backup paths that do not include said node and wherein one or more backup paths collectively have backup bandwidth greater than or equal to said bandwidth to be protected;

code that deducts, for each link included in said set of paths, from backup bandwidth available for protecting said node, while not deducting from backup bandwidth available for protecting other nodes in said data communication network; and

code that repeatedly invokes said code that identifies, establishes, and deducts for a plurality of link pairs connected to said node without exceeding available backup bandwidth of links used in establishing said backups;

wherein said bandwidth to be protected of said link pair comprises a lesser of primary bandwidths of links of said link pair traversing said node to be protected.

Claim 26 (canceled).

Claim 27 (canceled).

Claim 28 (original): The network device of claim 25 wherein said set of one or more paths comprises one or more label switched paths.

Claim 29 (original): The network device of claim 25 wherein said instructions further comprise:

code that signals said backups to other nodes adjacent to said node in said data communication network.

Claim 30 (currently amended): A network device for implementing a node in a communication network, said network device comprising:

a processor; and

a memory storing instruction for said processor, said instructions comprising:

code that maintains, for each of a plurality of links in said data communication network a primary bandwidth pool for use by primary paths and a backup bandwidth pool for use by backup tunnels; and

code that establishes said backup tunnels to protect a plurality of nodes of said network, each of said backup tunnels reserving backup bandwidth from backup bandwidth pools of selected ones of said plurality of links;

wherein all backup tunnels protecting any particular node of said network do not consume more bandwidth on any link than provided by the link's backup bandwidth pool but wherein there is at least one set of backup tunnels that protect disparate nodes and that consume more bandwidth on at least one link than provided by said at least one link's backup bandwidth pool;

wherein code that establishes backup tunnels comprises code that signals said backup tunnels with zero bandwidth to adjacent nodes of each protected node.

Claim 31 (original): The network device of claim 30 where at least one of said backup tunnels comprises a label switched path.

Claims 32-36 (canceled).

Claim 37 (new): The method of claim 1 wherein establishing a set of one or more backup paths comprises performing backup path selection computations at said node to be protected.

Claim 38 (new): The method of claim 1 further comprising dynamically adjusting said established backup paths in response to a change in one or more of said primary paths.

Claim 39 (new): The method of claim 1 wherein said backup paths are established at said node to be protected.

Claim 40 (new): The method of claim 1 further comprising signaling said one or more backup paths with zero bandwidth to one or more other nodes.

Claim 41 (new): The method of claim 8 further comprising identifying a failure at said node to be protected and rerouting traffic, wherein said traffic is rerouted in less than 50 milliseconds.

Claim 42 (new): The method of claim 8 wherein said primary bandwidth pool comprises a maximum amount of bandwidth that is available for allocation to primary paths.

Claim 43 (new): The method of claim 8 wherein said backup bandwidth pool comprises a maximum amount of bandwidth allocated for backup traffic.